MARK R. WARNER
VIRGINIA

United States Senate

WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

September 23, 2019

Andrei Soran, CEO
TridentUSA Health Services
930 Ridgebrook Rd.
Sparks Glencoe, MD 21152

Dear Mr. Soran,

It has come to my attention that one of your affiliated companies, MobileXUSA, recently left an unencrypted server online, exposing sensitive medical images and health data of Americans. According to recent reporting, researchers found 13.7 million data sets and 303.1 million images in medical image storage systems have been freely accessible online with no authentication requirements to access or download the images.[1] This left the MRI's, X-rays, and CT scans of millions of Americans exposed on the internet, not because of a breach, but simply because they were stored on 187 unprotected picture archiving and communication servers (PACS) including yours.[2] Additionally, along with the sensitive medical images, according to the research, your server displayed the names of more than a million patients.[3]

My colleagues and I in the Senate have been concerned about negligent cybersecurity practices in the health care space for a long time. Cybersecurity risks within the health care sector represent a growing threat, with 285 breaches reported between January and June of this year.[4] According to one report, there has been at least one healthcare-related data breach a day since 2016.[5] Just recently, the Senate Cybersecurity Caucus, of which I am a co-founder, convened a briefing that focused on healthcare and cybersecurity, particularly on the security of healthcare records which further highlighted the need for more robust cyber hygiene practices, and possibly additional standards.

It appears that the information held by MobileXUSA was made accessible due to sloppy cybersecurity practices— no software vulnerabilities were involved, and no explicit hacking was required. While HIPAA lays out some guidelines for secure data storage and transfer, it is not always clear who bears responsibility for securing the data and ensuring the use of proper controls. However, it is certainly the responsibility of companies like yours to control and secure sensitive medical data, maintain an audit trail of medical images, and to ensure the information is not publicly accessible.

To better understand how exactly millions of private medical scans were left open on the internet, I would appreciate your answers to the following questions:

---

[1] Cyber Resilience Report, Greenbone Networks GmbH, 2019. https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_EN.pdf
[2] Gillum, Jack, Kao, Jeff, Larson, Jeff. "Millions of Americans' Medical Images and Data are Available on the Internet. Anyone Can Take a Peek," September 17, 2019. https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet
[3] Ibid.
[4] Pifer, Rebecca. "Data breaches in 2019 already double all of last year," August 2 2019. https://www.healthcaredive.com/news/data-breaches-in-2019-already-double-all-of-last-year/560059/
[5] Ibid.

MARK R. WARNER
VIRGINIA

United States Senate

WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

1. HIPAA requires audit trails for PACS, which stores the data in centralized auditing databases with multiple audit layers. What audit and monitoring tools do you use to analyze the data to remain HIPAA compliant?
2. PAC server vulnerabilities are well known, however, their use of the DICOM protocol makes them easily accessible via the Internet. DICOM also enables PACS to communicate with neighboring systems in a medical or clinical process within a network of IP-enabled devices. Does your company require neighboring systems to comply with current standards and use access management controls?
3. What are your identity and access management controls for IP-addresses and/or port filters?
4. Do you require VPN or SSL to communicate with your PACS?
5. What is the frequency of your vulnerability scans and HIPAA-compliant audits?
6. What are your server encryption practices?
7. Do you have an internal security team or do you outsource it?

It is critical that the privacy of the individual– including their personal health information – is appropriately protected. I look forward to hearing your response by October 9th, 2019. Any further questions can be directed to Leisel Bogan in my office at Leisel_Bogan@warner.senate.gov

Sincerely,

Mark R Warner

Mark Warner
US Senator